Pragmatic Secure Design: Attack Surface Reduction

Shawn Hernan
Security Program Manager
Security Engineering and Communication

A Case Study: MS04-011

VULNERABILITY IDENTIFIERS	IMPACT OF VULNERABILITY	WINDOWS 2000	WINDOWS XP	WINDOWS SERVER 2003
LSASS Vulnerability - CAN-2003-0533	Remote Code Execution	Critical	Critical	Low
LDAP Vulnerability – CAN-2003-0663	Denial Of Service	Important	None	None
PCT Vulnerability - CAN-2003-0719	Remote Code Execution	Critical	Important	Low
Winlogon Vulnerability - CAN-2003-0806	Remote Code Execution	Moderate	Moderate	None
Metafile Vulnerability - CAN-2003-0906	Remote Code Execution	Critical	Critical	None
Help and Support Center Vulnerability - CAN-2003-0907	Remote Code Execution	None	Critical	Critical
Utility Manager Vulnerability - CAN-2003-0908	Privilege Elevation	Important	None	None
Windows Management Vulnerability - CAN-2003-0909	Privilege Elevation	None	Important	None
Local Descriptor Table Vulnerability - CAN-2003-0910	Privilege Elevation	Important	None	None
H.323 Vulnerability* - CAN-2004-0117	Remote Code Execution	Important	Important	Important
Virtual DOS Machine Vulnerability - CAN-2004-0118	Privilege Elevation	Important	None	None
Negotiate SSP Vulnerability - CAN-2004-0119	Remote Code Execution	Critical	Critical	Critical
SSL Vulnerability - CAN-2004-0120	Denial Of Service	Important	Important	Important
ASN.1 “Double Free” Vulnerability - CAN-2004-0123	Remote Code Execution	Critical	Critical	Critical
Aggregate Severity of All Vulnerabilities		***Critical***	***Critical***	***Critical***

Code fixed in Windows Server 2003 (50%)

Code not fixed in Windows Server 2003 (50%)

Extra Defense in Windows Server 2003 (29% of)

The Horrible Truth (1 of 4)

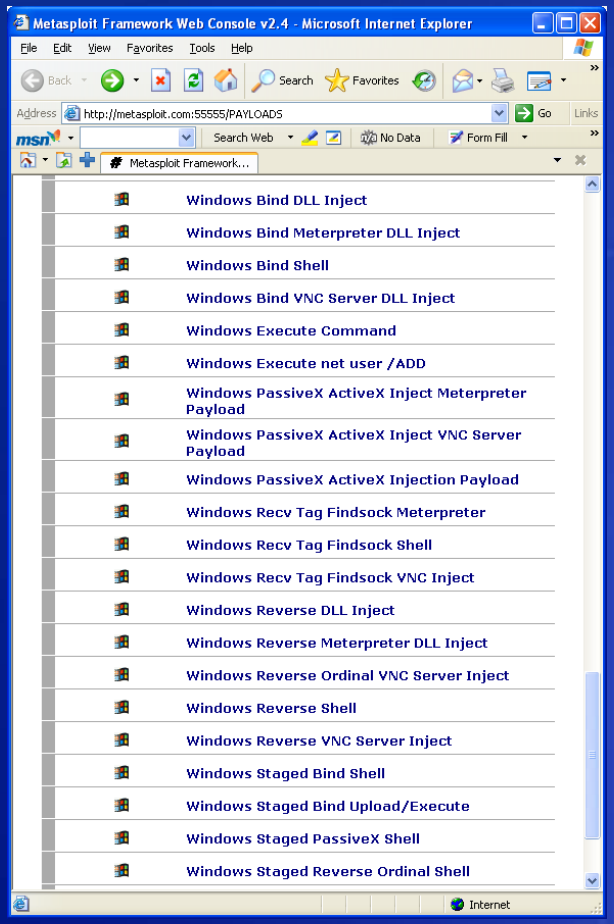
- No matter how much effort we expend, we will never get code 100% correct
  - Asymmetric problem
    - **We** must be 100% correct, 100% of the time, on a schedule, with limited resources, only knowing what we know today
      - Oh, and the product has to be reliable, supportable, compatible, manageable, affordable, accessible, usable, global, doable, deployable, …
    - **They** can spend as long as they like to find one bug, with the benefit of future research
  - We're human and our tools are far from

The Horrible Truth (2 of 4)

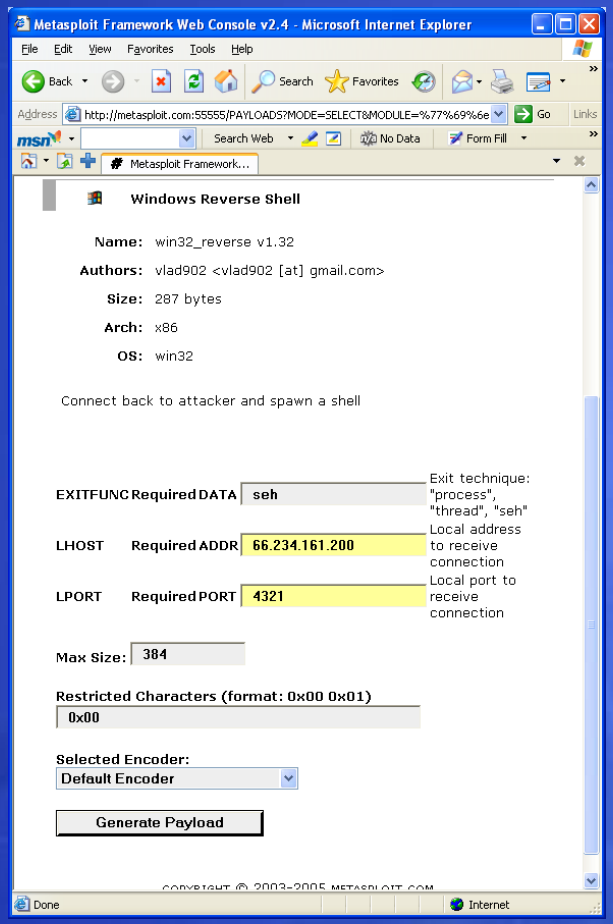
- The “Patch Window” is a joke
  - Once we issue a patch, the clock starts
  - “Zotob Proves Patching "Window" Non-Existent”
    - http://informationweek.com/story/showArticle.jhtml?articleID=168602115
    - “Defense in depth is your only chance to survive the early release of malware.”
  - “Hackers Beating Efforts to Patch Software Flaws”
    - http://www.computerworld.com/securitytopics/security/holes/story/0,10801,104092,00.html
    - “Instead of going out and looking for vulnerabilities on their [hackers] own, they are waiting for patches to be released to see what holes are being fixed." Then they go after those holes as quickly as they can. The trend could leave many companies dangerously exposed.”

The Horrible Truth (3 of 4)

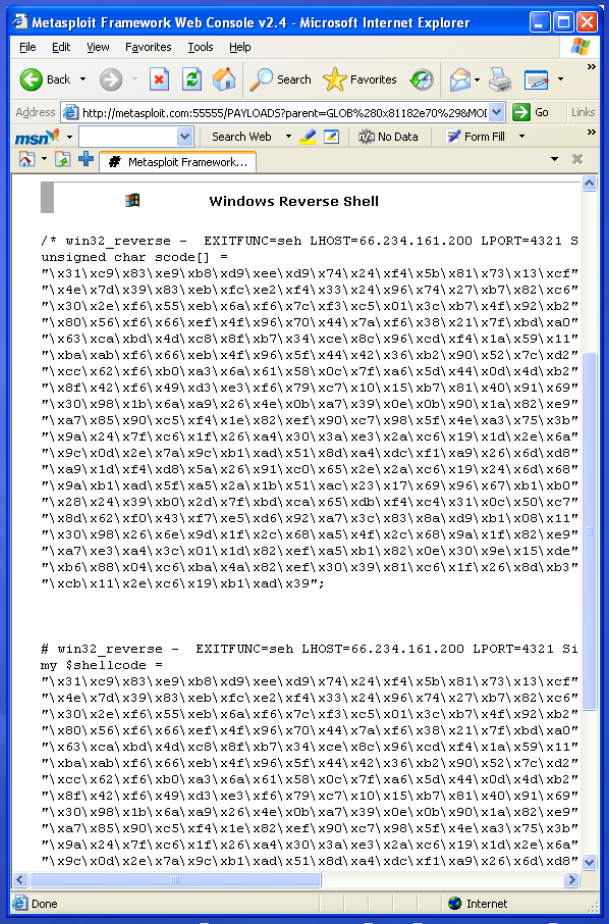
- Tools make it **easy** to build exploit code
- Reverse engineering tools
  - Structural Comparison of Executable Objects, Halvar Flake
    - http://www.sabre-security.com/files/dimva_paper2.pdf
    - PCT Bug: “Detecting and understanding the vulnerability took less than 30 minutes.”
    - H.323 ASN.1 Bug: “The total analysis took less than 3 hours time.”
- Exploit Payloads
  - www.metasploit.com



Choose your ‘sploit



Enter some details



Here’s the ‘sploit code!

The Horrible Truth (4 of 4)

- Cost for attacker to build attack is very low
- Cost to our customers is very high

The Attack Surface Reduction Process (1 of 2)

- Look at all your entry points (the threat model helps)
- Primarily network I/O and File I/O
- Can any of the entry points' attack surface be driven lower?

The Attack Surface Reduction Process (2 of 2)

Higher Attack Surface	Lower Attack Surface
Executing by default	Off by default
Open socket	Closed socket
UDP	TCP
Anonymous Access	User Access
User Access	Admin Access
Internet Access	Local Subnet Access
SYSTEM	Not SYSTEM!
Weak ACLs	Strong ACLs

Watch Out for Fanout!

- File formats
  - JPG, MSH, GIF, etc
- Sub-protocols
  - SSL2, SSL3, TLS, PCT
- Verbs
  - HTTP
    - Classic
      - GET, POST, HEAD
    - WebDAV
      - PROPPATCH, PROPFIND, DELETE, MOVE, LOCK
  - SMTP
    - HELO, EHLO, MAIL, RCPT
  - Queries
    - Extended sprocs, sprocs

ASR Examples

- Windows XP SP2
  - Authenticated RPC
  - Firewall on by default
- IIS6
  - Off by default
  - Network service by default
  - Static files by default
- SQL Server 2005
  - xp_cmdshell off by default
  - CLR and COM off by default
  - Network service
- Visual Studio 2005
  - Web server localhost only
  - SQL Server Express localhost only

How ASR Helped Microsoft Customers

- Sasser
  - Affected Win2000 and WinXP
  - Did not affect Win2003
    - RCP endpoint was marked local admin only
- Zotob
  - Affected Win2000
  - Did not affect WinXP
    - Firewall & authenticated RPC

Attack Surface Reduction is as important as trying to get the code right